IN THE CLAIMS

Amended claims follow:

1. (currently amended) A network bridge, said network bridge including a malware scanner;

wherein said network bridge is address-transparent with respect to data packets passing therethrough, such that at least in terms of addressing, no configuration changes are required when said network bridge is introduced in an associated network segment;

wherein, upon receipt of at least one of said data packets, said network bridge determines if said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received;

wherein, if it is determined that said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received, said at least one data packet is not passed by said network bridge;

wherein, if it is determined that said at least one data packet is not intended for a recipient on a side of said network bridge on which said at least one data packet was received, it is determined if said at least one data packet has a predetermined network layer protocol selected from the group consisting of TCP/IP; IPX; SNA; and Appletalk;

wherein, if it is determined that said at least one data packet has said predetermined network layer protocol, it is determined if said at least one data packet has a predetermined application layer protocol selected from the group consisting of SMTP; FTP; HTTP; SMB; and NFS;

wherein, if it is determined that said at least one data packet has said predetermined application layer protocol, portions of a data file from a plurality of said data packets are concatenated to form a data file to be scanned;

wherein, if it is determined that said at least one data packet does not have said predetermined application layer protocol, said at least one data packet is passed by said network bridge without being scanned.

2. – 7. (cancelled)

8. (original) A network bridge as claimed in claim 1, wherein said malware scanner is operable to scan for one or more of:

computer viruses;

Trojans;

worms;

banned computer programs; and

banned words within e-mail messages.

9. (original) A network bridge as claimed in claim 1, wherein data that has been scanned by said malware scanner is forwarded to its intended recipient.

10. (original) A network bridge as claimed in claim 1, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.

11. (currently amended) A network bridge comprising:

means for intercepting at least one data packet,

means for forwarding at least a portion of said at least one data packet to a malware scanner for scanning, and

means for forwarding data from said at least one data packet after scanning to an intended recipient;

wherein said network bridge is address-transparent with respect to data packets passing therethrough, such that at least in terms of addressing, no configuration changes are required when said network bridge is introduced in an associated network segment;

wherein, upon receipt of at least one of said data packets, said network bridge determines if said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received;

wherein, if it is determined that said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received, said at least one data packet is not passed by said network bridge;

wherein, if it is determined that said at least one data packet is not intended for a recipient on a side of said network bridge on which said at least one data packet was received, it is determined if said at least one data packet has a predetermined network layer protocol selected from the group consisting of TCP/IP; IPX; SNA; and Appletalk;

wherein, if it is determined that said at least one data packet has said predetermined network layer protocol, it is determined if said at least one data packet has a predetermined application layer protocol selected from the group consisting of SMTP; FTP; HTTP; SMB; and NFS;

wherein, if it is determined that said at least one data packet has said predetermined application layer protocol, portions of a data file from a plurality of said data packets are concatenated to form a data file to be scanned;

wherein, if it is determined that said at least one data packet does not have said predetermined application layer protocol, said at least one data packet is passed by said network bridge without being scanned.

12. – 16. (cancelled)

17. (currently amended) A malware scanner in combination with a network bridge, comprising:

means for receiving at least a portion of at least one data packet intercepted by said network bridge,

means for concatenating said at least one data packet into a data file to be scanned, and

means for forwarding said data file after scanning to an intended recipient via said network bridge;

wherein said network bridge is address-transparent with respect to data packets passing therethrough, such that at least in terms of addressing, no configuration changes are required when said network bridge is introduced in an associated network segment;

wherein, upon receipt of at least one of said data packets, said network bridge determines if said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received;

wherein, if it is determined that said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received, said at least one data packet is not passed by said network bridge;

wherein, if it is determined that said at least one data packet is not intended for a recipient on a side of said network bridge on which said at least one data packet was received, it is determined if said at least one data packet has a predetermined network layer protocol selected from the group consisting of TCP/IP; IPX; SNA; and Appletalk;

wherein, if it is determined that said at least one data packet has said predetermined network layer protocol, it is determined if said at least one data packet has a predetermined application layer protocol selected from the group consisting of SMTP; FTP; HTTP; SMB; and NFS;

wherein, if it is determined that said at least one data packet has said predetermined application layer protocol, portions of a data file from a plurality of said data packets are concatenated to form a data file to be scanned;

wherein, if it is determined that said at least one data packet does not have said predetermined application layer protocol, said at least one data packet is passed by said network bridge without being scanned.

18. (original) A malware scanner as claimed in claim 17, wherein said malware scanner is operable to scan for one or more of:

computer viruses;

Trojans;

worms;

banned computer programs; and

banned words within e-mail messages.

19. (original) A malware scanner as claimed in claim 17, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.

20. (currently amended) A method of malware scanning comprising the steps of:

receiving at least one data packet at a network bridge;

sending at least a portion of said at least one data packet from said network bridge to a malware scanner;

concatenating data received by said malware scanner to form a data file to be scanned;

scanning said data file with said malware scanner; and

forwarding said data file after scanning via said network bridge to an intended recipient;

wherein said network bridge is address-transparent with respect to data packets passing therethrough, such that at least in terms of addressing, no configuration changes are required when said network bridge is introduced in an associated network segment;

wherein, upon receipt of at least one of said data packets, said network bridge determines if said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received;

wherein, if it is determined that said at least one data packet is intended for a recipient on a side of said network bridge on which said at least one data packet was received, said at least one data packet is not passed by said network bridge;

wherein, if it is determined that said at least one data packet is not intended for a recipient on a side of said network bridge on which said at least one data packet was received, it is determined if said at least one data packet has a predetermined network layer protocol selected from the group consisting of TCP/IP; IPX; SNA; and Appletalk;

wherein, if it is determined that said at least one data packet has said predetermined network layer protocol, it is determined if said at least one data packet has a predetermined application layer protocol selected from the group consisting of SMTP; FTP; HTTP; SMB; and NFS;

wherein, if it is determined that said at least one data packet has said predetermined application layer protocol, portions of a data file from a plurality of said data packets are concatenated to form a data file to be scanned;

wherein, if it is determined that said at least one data packet does not have said predetermined application layer protocol, said at least one data packet is passed by said network bridge without being scanned.

21. – 25. (cancelled)

26. (original) A method as claimed in claim 20, wherein said scanning scans for one or more of:

computer viruses;

Trojans;

worms;

banned computer programs; and

banned words within e-mail messages.

27. (original) A method as claimed in claim 20, wherein said malware scanner is formed of one or more of:

a software based malware scanner; and

a hardware based malware scanner.

28. (new) A network bridge as claimed in claim 1, wherein said network bridge includes a pair of network interface units that operate to receive said data packets on an associated network line and pass said at least one data packet to a packet analysis unit connected thereto, said packet analysis unit coupled to a software based malware scanner and a hardware based malware scanner.

29. (new) A network bridge as claimed in claim 1, wherein a plurality of said malware scanners is included with said network bridge, each malware scanner adapted for handling different predetermined network layer protocols and different predetermined application layer protocols, where said malware scanners are passed said at least one data packet based on said determination whether said at least one data packet has said predetermined network layer protocol and said determination whether said at least one data packet has said predetermined application layer protocol.

30. (new) A network bridge as claimed in claim 1, wherein, after scanning, a data file is broken down into said data packets for forwarding to an intended recipient.